

3－2 導入課題に関するヒアリング結果

次に、「導入課題」に関するヒアリング結果を示す。

なお、有識者ごとの主な質問項目は以下のとおりである。

有識者		質問項目
関口 忠	前：行政情報システム研究所 客員研究員	1. 自治体のネットワーク分離がもたらす制約 2. ネットワーク分離に伴うクラウド型AIサービス利用にあたっての論点
石井 夏生利	筑波大学図書館情報メディア系 准教授、弁護士	1. AIやデータ利活用に伴う法的リスク 2. GDPR（一般データ保護規則）の影響 3. 今後の課題

1. 関口 忠 [前：行政情報システム研究所 客員研究員]

(資料編) 図表3-1 クラウド型 AI サービスの利用条件

本編第5章第4節5.(1)「①ネットワークセキュリティ等の制約」に関して、1.自治体のネットワーク分離がもたらす制約、2.ネットワーク分離に伴うクラウド型 AI サービス利用にあたっての論点をまとめた、クラウド型 AI サービスの利用条件は以下のとおりである。

	①基幹系 (マイナンバー利用 事務系)	②L GWAN接続系	③インターネット接続系
利用可能な データ (想定)	マイナンバー対象業務の データ (4業務)	①③以外の業務用データ 全般 (その他の業務データ)	公開可能データ
クラウド型 AIサービスを利用する 前提条件	不可	L GWAN-ASP上に 当該サービスが登録され ること	- 最新のセキュリティ対策を 施したネットワーク環境を 整備すること - 当該サービスの利用条件等 を確認の上、各自治体の規 定に準じて例外申請等の手 続きを行うこと
クラウド型 AIサービスを利用する 制約条件	-	- 事業者にとってはメリッ トがなければ提供され ない - 複数自治体が汎用的に 利用するサービスでな ければ事業者から提供 されにくい	- 自治体ごとのセキュリティ 対策によっては、対象端末 数及び帯域等の制約がある こと - 自治体が個別にサービスの 利用可否を判断する必要が あること - 自治体によって接続を許す 基盤や手続きが異なり、手 続きそのものが制約となる こと

基幹系 (マイナンバー
利用事務系) と他の接
続系領域との通信は
原則不可

自治体ごとにL GWAN
接続系とインターネット
接続系との無言化通
信に係るルールや方法
が異なる

2. 石井 夏生利 [筑波大学図書館情報メディア系 准教授、弁護士]

議 事 概 要			
日 時	2018 年 9 月 25 日 (火) 15:00～16:20	場 所	行政情報システム研究所 会議室
参加者 (敬称略)	[筑波大学]図書館情報メディア系 石井准教授 (聴取者) [東京市町村自治調査会] 岸野、秋野 [行政情報システム研究所] 狩野、松岡、栗田		
1. AI やデータ活用に伴う法的リスク			
(1) 本人が識別され得る場合 本人が識別され得るような情報を利用する場合に、どのような点に留意が必要か？			
① 住民からの問合せに対し、自治体が個々の住民にパーソナライズ化した回答を提供する目的で登録済の本人情報を利用する場合			
・ 個人情報情報の事務目的以外での利用に該当するか否かの確認が必要。それに当たるかどうかは、各自治体の条例が目的外利用をどのように定めているかによる。神奈川県など、本人に提供する場合本人の同意があるのと同じであるため、許される旨の規定を置いている自治体もある (ただし、自己情報の開示請求との関係整理が必要)。住民との接点がある<u>事業であるため</u>、まずは問合せを受けた時点で、本人から直接同意を取るのが安全な方法(リスクヘッジ)である。			
② 道に迷ってしまった認知症の住民について、他の住民が当人を撮影した画像を自治体へ送付して本人照合する場合 (親族の同意あり)			
・ ①以前から保有している住民情報の目的外利用と、②本人に関する情報の新たな取得について、条例の規制を確認する必要がある。 ・ 本人に判断能力がなければ法定代理人から同意を取る必要がある。ただ、法定代理人がおらず、本人能力が不十分な場合は、親族の同意で代替するしかない。 ・ 参考までに、市川市など、防犯カメラについての特別な条例や規程を置いている自治体が多い。			

・ 新たな事務登録を要するかの確認も必要。 ・ 本人外収集や本人通知の省略について、個人情報保護の審議会で議論される場合がある。また、審議会事実といえるか否かが微妙な事案についても、安全策を取る観点から審議会にかける例も見られる。条例に照らして個人情報保護に関する判断を行う。 ・ 参考までに、防犯カメラの場合は、利用目的を公表するための表示(防犯カメラ設置中であることや、その他透明性を高めるための措置が望ましい(例：撮影時間、画像の処理の仕方、問合せ先 等))。 ③ 自治体が個々の住民にパーソナライズ化した情報を発信するため、自治体サイトへの住民のアクセスログ等を分析する場合	・ アクセスログが本人と紐づく場合には個人情報に当たる。まずは情報収集時の規制を確認する。次に、情報の解析が、個人情報を取り扱う事務の目的の範囲内といえるか否かが問題。目的外利用の場合は、本人同意を得ることや、審議会にかけることで取り扱うことを認める自治体がある(条例上、目的外利用が認められる場合の要件を要確認)。 ・ アクセスログの分析を事務目的外で行う場合に、本人の個別同意を取得する機会がなければ、他の例外規定を用いる必要がある。例えば、同一実施機関内の利用であれば、「事務に必要な限度で利用し、かつ、利用することに相当な理由がある」と認められるとき」といった規定を置いている自治体もある(東京都)。本人が受けられる福祉サービスの提供を効率的に提供するような場合は抵抗感もないであろうが、それ以外は住民の抵抗感が大きいことも想定される。そのため、オプトアウトを設けるなど、個々の住民の意向が反映できる対応も必要となる。 ・ 個人情報の利用にあたり本人の同意を取得することが、一番の裏付けとなる(有効期限もなく、適法性の担保も容易)。住民へ説明すべきことは、利用目的(公益性があること)、条例の根拠があること、及び本人が利用拒否できることなどである。また、窓口で本人の同意を得た場合など、個人情報を利用する段階で個別に伝える場合と、パーソナライズ化したサービスの開始に際して事前に一律に周知する場合とで、説明すべき内容、方法が異なる。 ・ 個人情報を利用する場合には、個人情報保護条例に抵触しないかという点と、住民がハレーション(拒否反応)を起こさないかという点に配慮する必要がある。 (2) 本人が識別できない場合 本人を識別できないが個人の行動等に関する情報を利用する場合に、どのような点に留意が必要か？
--	---

① 来庁者をカメラで撮影し、トラブルの早期発見等のために表情を分析する場合	・ 来庁者をカメラで撮影した時点で、個人情報に該当する。つまり、当人であることが分かる画像は、個人を識別可能な情報である。そのため、IT機器が本人を識別する処理を行わなくても、画像を取得した時点で個人情報を保有することになる。したがって、カメラを利用する場合は、予めどのように利用するか説明しておくことや、取得した画像をどのように管理するかが問われる。本来は撮影される側に事前の同意を得るべきではあるが、実際上、同意の取得は困難なので、透明性を高めるための措置として、カメラ設置中であること、撮影時間、画像の処理の仕方、問合せ先等を目につく場所へ示すのも一案である。IoT推進コンソーシアムが監視カメラの画像の扱いに関して表示すべき事項など一定の指針を設けている。カメラ画像の保護と利活用に関するシンポジウムの成果もまとめられている。 ② 不特定多数の人の映像や画像を撮影し、混雑の予測や避難誘導等に利用する場合 ・ 近年のカメラは非常に精度が高く、不特定多数の人であっても、顔の映像や画像を撮影した時点で、原則として個人情報に該当する。つまり、当該ケースの画像についても、個人識別性があると考えられる。避難誘導のケースについては、NICT(独立行政法人情報通信機構)が4-5年前に大阪で実験を行おうとしたが、反対意見が出て問題になった事案がある。実証実験においては参加者の同意を取得できるが、実際の運用となると不特定多数の中で同意しない人が出てくることがあるので難しい。 ・ ただし、シルエット画像等による移動軌跡データ(人流データ)は、他の情報と照合できなければ個人情報でないと解釈されている。 ・ ①と②のカメラの関係については、条例・規程上の根拠を設けることが望ましいのではないか。また、これらの施策の必要性や正当性を説明し、利用の透明性を高めることが必要となる。 ③ 住民、職員の健康情報や、人事上の適性評価情報等を匿名化してAIの学習データとして利用し、他者向けの提案等に用いる場合 ・ 健康情報は、センシティブな情報のため、取扱注意である。情報の種類によっては、取扱いによってバイアスがかかることで差別的になり、人格権や個人の尊厳を侵害するおそれがある。これには2面があり、1つは他人の情報を元に自分が評価されたときに不本意な評価を受けて人格権侵害となる場合と、もう1つは自分の情報が他人のために使われることを想定していない場合である。もちろん、自分の情報が自分の評価のために解析され、予想外の結果を出される例が典型である。 ・ 自治体の条例は、職員ではなく地域住民の保護を趣旨としたものが多いのではない。
---	---

- 取得した情報の匿名化処理を行っても、ID が割り振られている場合などで、再び実施機関内で再識別が可能となった場合、問題視される可能性がある。収集した情報を匿名化した組織と加工した情報を利用する組織が別である場合、利用側の組織で、他の情報と照合しても個人の識別が不可能であれば、提供を受けた情報は個人情報には当たらないという解釈となる。ただし、匿名化は識者によっては異論の出やすいところである。一切のID その他の紐付け可能な情報を消去し、どの組織においても完全に個人識別性がなくなれば別だが、注意が必要なケースである。 - 面談の内容は、そもそも機密性が高い性格を有しており、利用に際しては特段の注意が必要。逆に情報利用の同意を得ようとすれば、面談で話がしにくくなるという懸念もあるのではない。 - 健康情報や人事上の適性評価情報等を利用し、個人の評価に用いる場合は、判断の結果が説明できること、その結果に納得がいかない者の苦情申出先が必要。個人の評価に用いない場合は、職員健康管理に伴い特定の傾向を事前に察知する仕組みなど、社会全体の利益につながるような用途を考えるべき。 (3) 過失に関するもの	- チャットボットが誤解を招きかねない回答をした結果、住民に損失（機会損失など）が発生した場合、自治体はどのような責任を問われるか？ - 具体例をもとに考えるべきであるが、学習データの誤入力によりAIが不適切な判断をし、自治体が判断を正す手続を設けず、住民が受けられるはずの行政サービスを拒否されたような場合には、不作為に対する責任が生じ得る。AIに誤りが生じないための技術的処理をできる限り行うべき。計算方法と用いる情報について、説明を求められる可能性がある。不服を申し立てられる手続も必要。また、クレーム等が生じる可能性は否定できないが、実際には個別に再受付等の対応をすれば問題は深刻化しないのではない。 - このような事象が生じれば、チャットボットの精度は問われるであろう。また、利用者の誤解を招かないようなインタフェースの品質も必要だと言えるであろう。 - 音声データに一部個人情報を含む場合や、個人を識別可能な画像データを庁外のクラウド上のAIサービスに送信することには、どのような法的リスクを伴うか？ - 契約条項と、委託先であるクラウドにおける情報の管理状況をできる限り確認する必要がある。庁外のクラウドが個人情報を取り扱わなければ（単に預けるだけであれば）、自治体の管理外に移転したことにはならない。 - 国内のサーバーの使用を事実上義務付けた運用もなされているであろうが、海外のサーバー
---	---

を利用する場合は国内法が及ばないことや、当該外国の法に基づき、海外サーバーに置いたデータが集められてしまうという面でリスクはある。契約によってクラウドサーバーに保存されたデータを扱わないようにする規定や、国内サーバーに限定する方法もあるが、クラウドにおける情報の管理状況をできる限り確認することは必要である。他方、情報の安全性という意味では、人材面で庁内監理が安全とも言い切れない。情報管理の状況確認を怠れば責任を問われる可能性があるため、クラウドを利用する場合には、クラウド事業者の信頼性を十分評価することが重要である。	(4) その他 ① 自治体職員によるウェブ検索やメール等のログから解析した興味、関心事項を業務の効率性の向上（例：レコメンド）のために活用する場合、どのような点に留意が必要か？ - 職場といえども私的な環境は守られるべきである。本件は従業員の監視であるとして争われた例がある（従業員側が敗訴）。職務専念義務を果たさせるために、社会通念上（常識）の適切な範囲であれば監視も認められるであろうが、この場合はそれに当たらない。少なくとも、予め組織規程を定め、従業員への周知及び必要に応じて労使が話し合えるという条件を整える必要があるであろう。本人が解析を望まない場合はオプトアウトできるようにする仕組みも必要である。 - 保育所や移住等の申請に対する判断を AI に委ね、希望にそぐわない結果となった場合、どこまで説明責任が求められるか（ルール、アルゴリズム、パラメータ等）？ - アルゴリズムの説明までは不要であると言われている。説明すべき内容は、判断のもととなった情報（データ）、評価指標（パラメータ）、評価の結果がどうなったか（結果）、である。プログラムに明るくない文系タイプにも、判断の根拠が分かるような説明が求められる。ほぼ同じ条件の住民がいた場合に、異なる結果が生じた場合、不利益判断を受けた住民からその理由の説明を求められたときに答えられることが必要。この問題は、プライバシーや個人情報を超える問題につながる。 - AI の利活用に対して法的な懸念が多いように感じるかもしれないが、AI といえばプロファイリング、プロファイリングといえ個人情報、という連想があるためである。人の情報を処理することは、何かしらの人の評価につながる。それはまさにプロファイリングの問題と言える。GDPR の考え方では、プロファイリングという手法の処理に異議を申し立てる権利と、不利益結果に服さなくて良い権利がある。GDPR の思想は、個人情報を機械が扱うことは良くないという思想に基づいている。プロファイリングは個人情報保護法改正の継続的な検討課題となっている。それは、誰もがパーソナライズ化を望んでいるとは限らないからである。 - 個人情報の利用を懸念する人が、自治体がつつ本人の情報を確認するため、個人情報
--	---

の開示請求を行うことも考えられる。開示は、本来的に持っている情報をそのまま出すという仕組みであるから、当人の申請事項を始めとする基本情報、AIによる処理方法、判断結果を一体の文書として示すことになるのではないか。個人情報の利用が事務目的内であるか、利用方法が非難されるようなものでないか、という観点が必要である。住民生活を上させるための使い方を模索すべきで、住民に納得してもらえなかろうかに尽きる。公益性のある使い方であれば、個人情報保護の観点からも容認すべき場面はあるように思われる。

2. GDPR(一般データ保護規則)の影響

① EU内の居住者が日本の自治体の行政サービスに登録したデータの取扱いに関して、GDPRとの関係でどのような点に留意が必要か？

- ・ GDPRに関する十分性の合意は、EUからの越境データ移転に関する枠組である(注：2019年1月23日に十分性認定が承認された)。他方、十分性とは異なり、国外の事業者等が直接にGDPRの適用を受ける場合がある。日本の自治体がEUの居住者に行政サービスを行い、その情報について分析したり行動を監視等すれば、GDPRを適用される可能性はある、というのが基本的な解釈である。
- ・ しかし、日本の自治体がEUに居住する日本人のデータを扱う事業は想定しにくいのではない。GDPRの規定は、官民双方に適用されるが、GAFAのようにEU内の居住者のデータを使って儲けることを抑止することを1つの狙いとしており、民間規制の議論が目立つ印象ではある。EU市民に向けて広告を行ったり、ユーロでの商品・サービス取引等の場面に主に想定されている。また、EU内に派遣した人を評価分析する場合もあるが、この場合にGDPRが適用されるという見解もある。収集後の行動分析又はプロファイリングを行うかどうかという点がメルクマールとなる。
- ・ そもそも十分性の合意は、民間の個人情報保護法だけを対象としていて、行政機関は対象としておらず、部分的なものである。したがって、自治体のサービスや行政機関は手が付けられていないと考えられる。継続的な留意は必要だがリスクは低いのではない。

3. 今後の課題

① 自治体におけるAI導入の進展に伴い、今後顕在化し得る法的リスクとして、どのような点に留意が必要か？

- ・ AIがブラックボックスであるが故に説明責任を果たせるかという点は、リスクになると思う。AIが行った職員の評価をどこまで説明できるか。判断はAIで完結することなく、本人に不満があるならば、その不満を申し出る先を用意し、最後は人が行うべきである。判断

のペースとなったデータと評価指標は説明する必要がある。

- ② 上記のリスクに対して、今後、自治体においてどのような対応が求められるか？
- ・ AIの適用は、地域社会全体に役に立つことに利用する、できる限り同意を取る、基本となったデータと評価指標は明確にする、ということが前提である。個別の事案については、自治体の条例がどのように適用されるかという視点が重要である。必要に応じて、AIの利活用に関する規定を設けることも考えられる。その場合は、用途を限定して導入しながら規程を定め、徐々に対象を広げていくと良い。

以上

(資料編) 図表 3-2 導入課題に関するヒアリング結果

ヒアリングにあたり事前に「想定する活用例」を設定し、石井氏の発言を活用例ごとの「課題・問題点」としてまとめた。また、石井氏の発言をもとに「AI 固有の課題」及び「活用例を実現するに当たっての影響」かどうかについて区分づけを行った。

項番	想定する活用例	課題・問題点	AI固有の課題	活用例を実現するに当たっての影響	根拠 (左記影響の大きさについて)
1	住民からの問合せに対し、自治体が個々の住民にパーソナライズした回答を提供する	条例に照らして、本人に関する情報の利用が個人情報の目的外利用に該当するか判断が必要。神奈川県など、本人に提供する場合は同意があるのと同じであるため、許される旨の規定を置いている自治体もあるのではないかと(ただ、自己情報の開示請求との関係整理が必要)。	○	中	一般的な個人情報保護に係る手続きの範疇であるため。
2	道に迷った認知症の住民について、他の住民が当人を撮影した画像を自治体に送付して本人照合する	①以前から保有している住民情報の目的外利用と、②本人に関する情報の新たな取得(目的の明確化、適法公正な手段等)について、条例の規制を確認する必要がある。条例が本人収集を原則としているかどうかとも確認が必要。	-	小	本人能力が不十分であれば法定代理人や親族の同意で代替する。
3	自治体が個々の住民にパーソナライズした情報を発信するため、自治体サイトへの住民のアクセスログ等を分析する	アクセスログが本人と紐づく場合には個人情報に当たる。まずは情報収集時の規制を確認する。次に、情報の解析が、個人情報を取り扱う事務の目的の範囲内といえるかが問題。目的外利用の場合は、本人同意を得ることや、審議会にかけることを取り扱うことを認める自治体がある(条例上、目的外利用が認められる場合の要件を要確認)。	○	大	個人情報保護に係る手続きが必要であり、かつ行政サービスの効率的な提供に直結しない場合は住民の抵抗感が大きくなる可能性があるため。
4	来庁者をカメラで撮影し、トラブルの早期発見等のために表情を分析する	・顔画像は個人情報に該当する。防犯カメラの取扱いに関する条例や規程を置いている自治体が多い。 ・条例の定めによるが、利用目的を公表するための表示(防犯カメラ設置中であること)や、その他透明性を高めるための措置が望ましいのではないかと(例：撮影時間、画像の処理の仕方、問合せ先 等)。マルチユースの場合は防犯以外の目的に使うことを示す必要がある。	-	中	一般的な個人情報保護に係る手続きの範疇であるため。
5	不特定多数の人の映像や画像を撮影し、混雑の予測や避難誘導等に利用する	撮影情報が特定個人を識別できる程度の精度であるか否かによって、個人情報性は異なる。シルエット画像等による移動軌跡データ(人流データ)は、他の情報と照合できなければ個人情報でない。個人を識別できる場合、撮影時は上記と同じように、利用目的の公表等を行う必要がある。その後の利用は、本人を識別できる形で利用するか否かによる。	○	中	一般的な個人情報保護に係る手続きの範疇であるため。
6	住民、職員の健康情報や、人事上の適性評価情報等を匿名化してAIの学習データとして利用し、他者向けの提案等に用いる	・人の情報の分類は差別的に用いられるおそれがある(プロファイリング) ・社会的差別の原因となる情報を収集することを規制している自治体もある。 ・他人の情報をもとに不本意な評価を受けると、人格権侵害とされる場合がある ・自身の個人情報がある他人のために使われることを想定していない場合は個人情報保護も課題。ただし、自治体の条例は、職員ではなく地域住民の情報保護を意図して作られているのではないかと。 ・他方、個人情報利用の事前同意を得ようとするれば、面談本来の目的が果たせなくなる懸念が生じる。	○	大	情報の匿名化処理においてIDが割り振られる場合など、識別が可能な状態であれば問題視される可能性があるため。個人情報保護の問題のみならず、人権や人格権侵害にわたる可能性があるため。
7	音声データに一部個人情報を含む場合や、個人を識別可能な画像データを庁外のクラウド上のAIサービスに送信する	・契約条項と、委託先であるクラウドにおける情報の管理状況をできる限り確認する必要がある。庁外のクラウドが個人情報を取り扱わなければ(単に預けるだけであれば)、自治体の管理外に移転したことはならない。なお、調達の際のセキュリティポリシー上、国外のデータセンターでの処理は制限されているのではないかと。	○	小	・データを庁外のクラウドに送信するからといって、法的にリスクが高まるとは言えない。 ・画像等の公開前に内容をチェックする用途は、個人情報保護上の安全管理措置の一環またはプライバシー侵害を避けるための措置として考えることができるため。
8	自治体職員によるウェブ検索やメール等のログから解析した興味、関心事項を業務の効率性の向上(例：レコメンド)のために活用する	メール監視がプライバシー侵害として争われた例がある。レコメンドは個人情報の安全管理措置の一環とはいえない。個別に同意を得る形が望ましいのではないかと。	-	中	一般的な個人情報保護に係る手続きの範疇であるため。
9	住民からの申請や問合せに対し、AIが判断して回答する	・学習データの誤入力によりAIが不適切な判断をし、自治体が判断を正す手続を設けず、住民が受けられるはずの行政サービスを拒否されたような場合には、不作為に対する責任が生じ得る。 ・AIの判断が不適切とはいえず、自治体の過失に該当しない場合であっても、AIに誤りが生じないための技術的処理をできる限り行うべき。計算方法と用いる情報について、説明を求められる可能性がある。不服を申し立てられる手続も必要。 ※学習データやプログラム次第で、適切な深層学習を実施したはずのAIであっても、誤判断する可能性はある。	●	小	・申請に対する誤判断に対しては、個別に再受付等の対応をすれば問題化はしない可能性があるため。 ・利用者の誤解を招かないようなAIのインタフェースの品質は必要となるため。 (深層学習を実施したAIの誤判断を、AI固有の課題として含めた)
10	保育所や移住等の申請に対する判断をAIに委ねる	プロファイリング問題と重なるのではないかと(項番6参照)。	○	大	どういう情報から判断したのか(データ)、どういう評価指標であるか(パラメータ)、その結果どうなったかを説明できることが求められるため。

凡例 ○：AIを利用したサービス固有の課題 ●：○のうちAIプログラムの処理に根拠した固有の課題 -：左記に該当しない課題（一般的な課題）